Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2017

2017. gada 3. ceturksnis (01.07.2017. – 30.09.2017.)

Pārskatā iekļauta vispārpieejama informācija, tas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Saturs

Kopsavilkums

Pārskata periodā vairāki uzņēmumi un valsts un pašvaldību iestādes saņēma krāpnieciskus e-pastus, kas sūtīti uzņēmuma vai iestādes grāmatvedei organizācijas vadītāja vārdā ar lūgumu veikt steidzamu bankas pārskaitījumu. Visos gadījumos e-pasti tika identificēti kā krāpnieciski (*CEO fraud*) un zaudējumi netika nodarīti.

Augustā tika saņemts kārtējais ziņojums par nelicenzētas finanšu platformas *Grand Capital META4* darbību, kuras izmantošana lietotājam radīja 2600 eiro lielus zaudējumus.

CERT.LV uzmanības lokā nonāca arī krāpšana sociālajā tīklā *Facebook*, kurā krāpnieki uzrunāja upurus it kā ar mērķi iepazīties, lai pēcāk iežēlinātu tos un mēģinātu izspiest no upuriem naudu.

Visa perioda garumā CERT.LV aktīvi gatavojās Eiropas Kiberdrošības mēnesi ievadošajam pasākumam Latvijā – kiberdrošības konferencei „Kiberšahs 2017", apzinot runātājus, gatavojot programmu, organizējot pieteikšanos un veicot citus organizatoriskos darbus. Šogad konference piedzīvoja rekordlielu interesi: pieteikumu limits tika izsmelts pirmajās četrās pieteikšanās dienās.

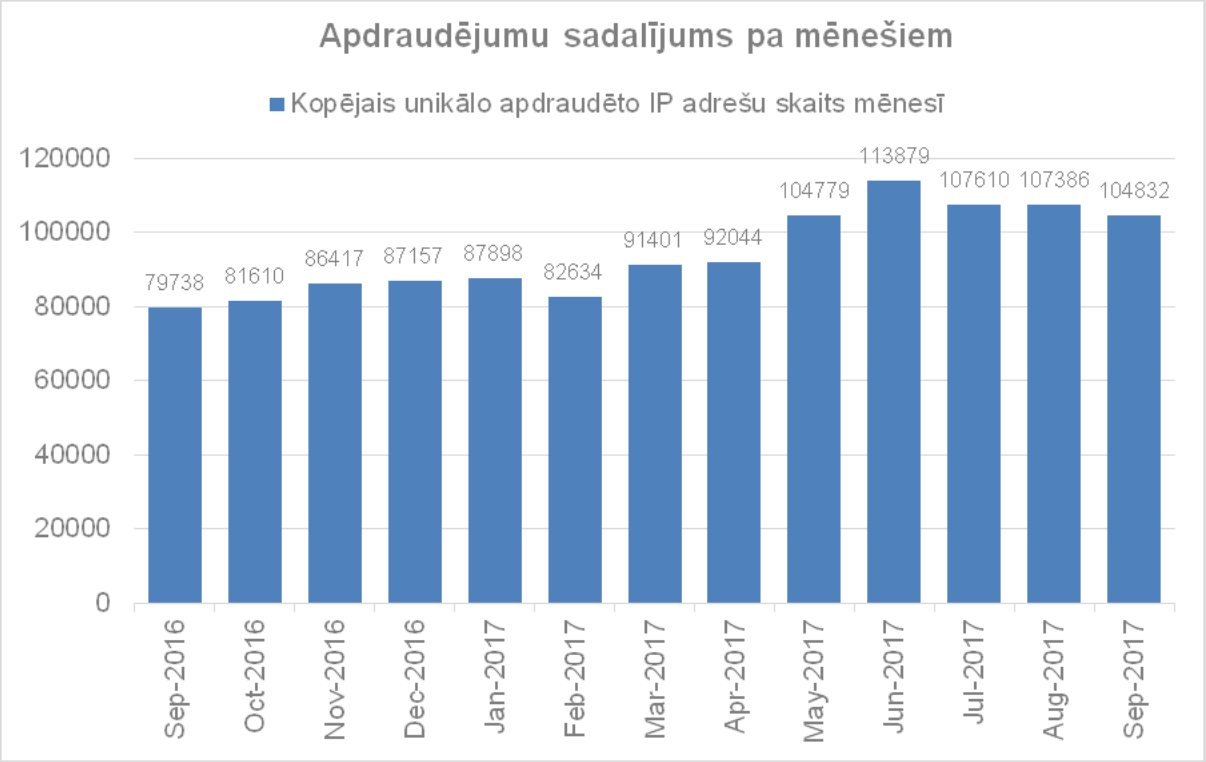
2017.gada 3.ceturksnī CERT.LV apkopoja informāciju par 208 076 apdraudētām IP adresēm. Pārskata periodā izplatītākais apdraudējums bija konfigurācijas nepilnības (141 316 unikālas IP adreses) ar kritumu 6%, salīdzinot ar iepriekšējo ceturksni. Nākamais izplatītākais apdraudējums bija ļaundabīgs kods (57 084 unikālas IP adreses) ar pieaugumu 37%. Trešo vietu ieņēma ielaušanās mēģinājumi (182 unikālas IP adreses) ar kritumu 3% attiecībā pret iepriekšējo ceturksni.

Pārskata periodā CERT.LV par IT drošību izglītoja 625 cilvēkus, iesaistoties 13 izglītojošos pasākumos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, no 2017. gada 1. janvāra apdraudējumu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija). Turpmāk statistikā visi CERT.LV reģistrētie apdraudējumi tiks uzskaitīt vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa infekciju (piemēram, *Confiker*, *Zeus*, Mirai) un ievainojamību (piemēram, *Opendns*, *Openrdp*) tipiem.

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 100 000 – 110 000 ievainojamu unikālu IP adrešu.

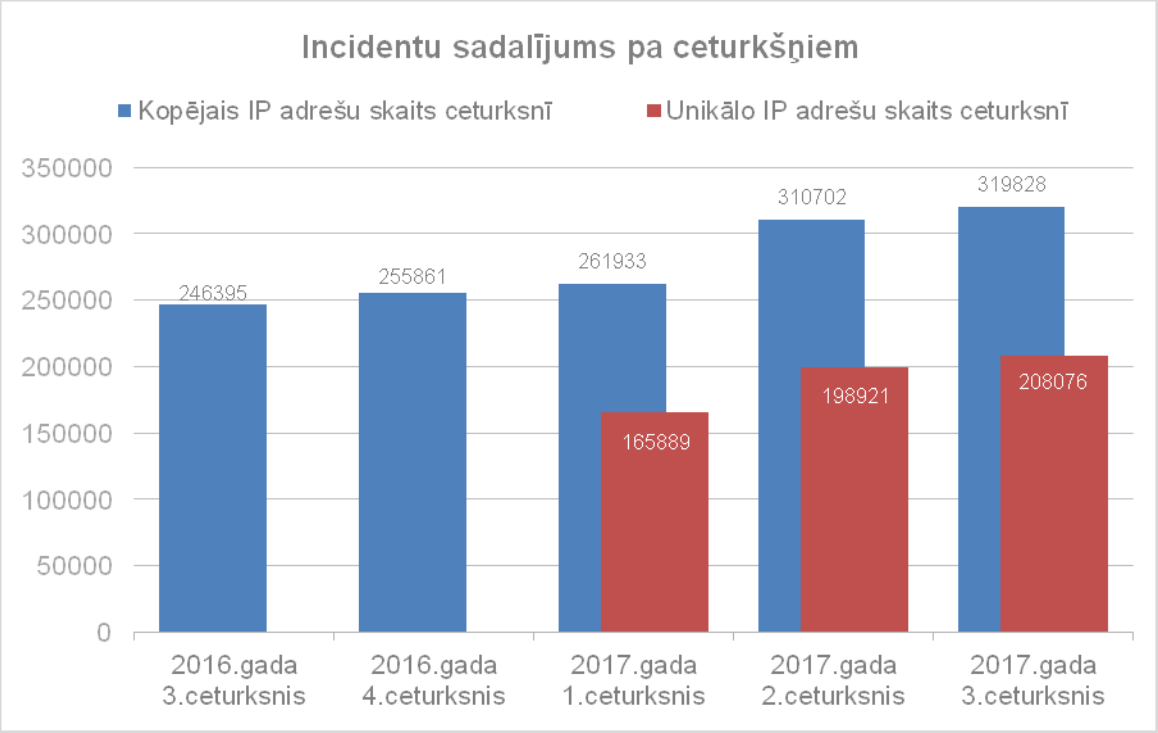


1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

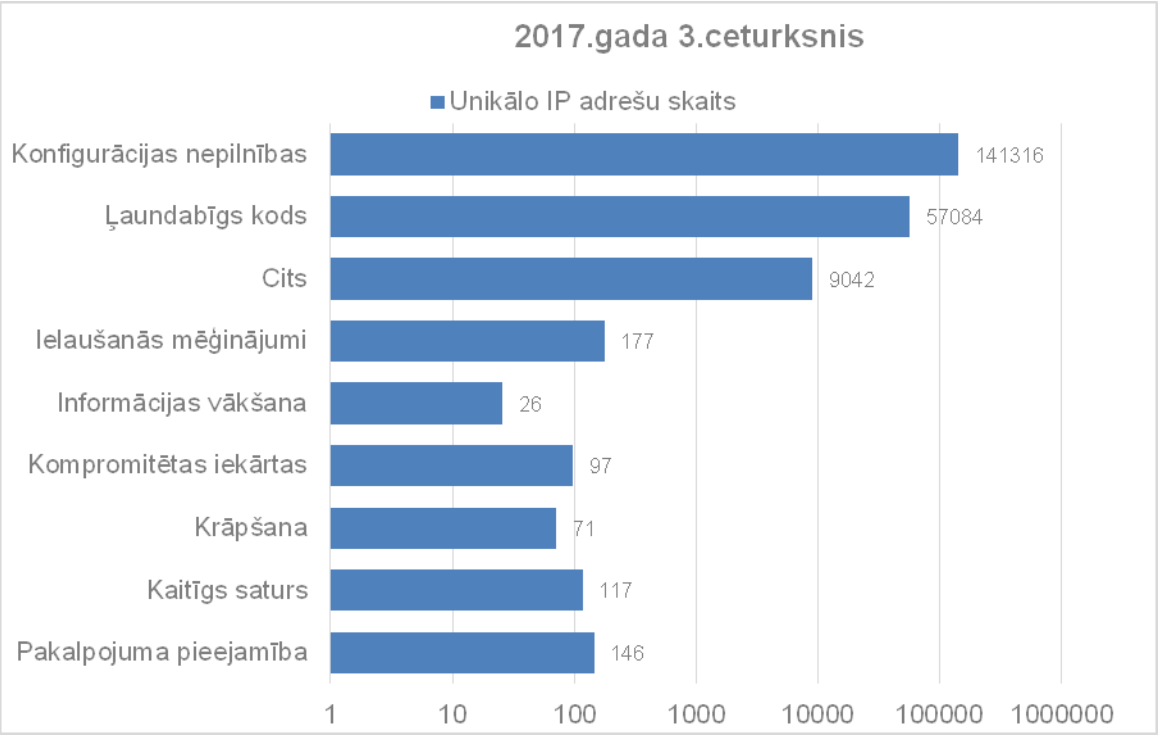
Pārskata periodā nav vērojamas būtiskas izmaiņas mēnesī reģistrēto apdraudēto IP adrešu daudzumā.

Līdz 2016. gada beigām CERT.LV apkopoja informāciju par ceturksnī apdraudētajām IP adresēm, summējot katrā mēnesī apdraudētās IP adreses (2. attēls – zilie stabiņi). No 2017. gada janvāra CERT.LV veic uzskaiti pa unikālām IP adresēm ceturksnī, novēršot to, ka viena un tā pati IP adrese tiek pieskaitīta vairākas reizes (2. attēls – sarkanie stabiņi).

2017. gada 3. ceturksnī tika reģistrētas 208 076 unikālas apdraudētas IP adreses (izmantojot iepriekšējo metodi, tās būtu 319 828 IP adreses). Skaita atšķirība norāda uz to, ka vienas un tās pašas adreses tiek reģistrētas, kā apdraudētas vairāku mēnešu garumā, jo apdraudējums netiek ilgstoši novērsts vai atkārtojas.

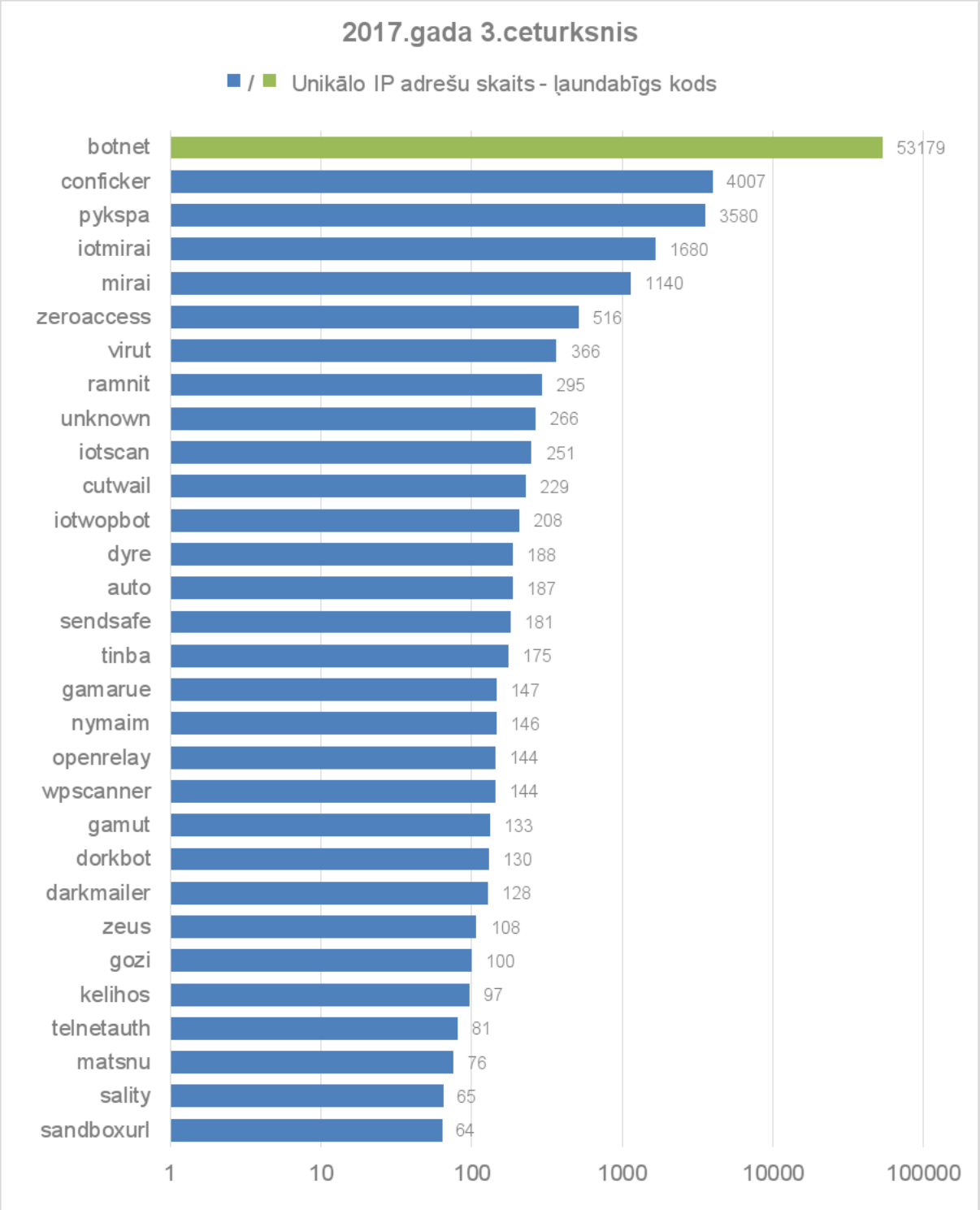


2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2016. un 2017. gadā.



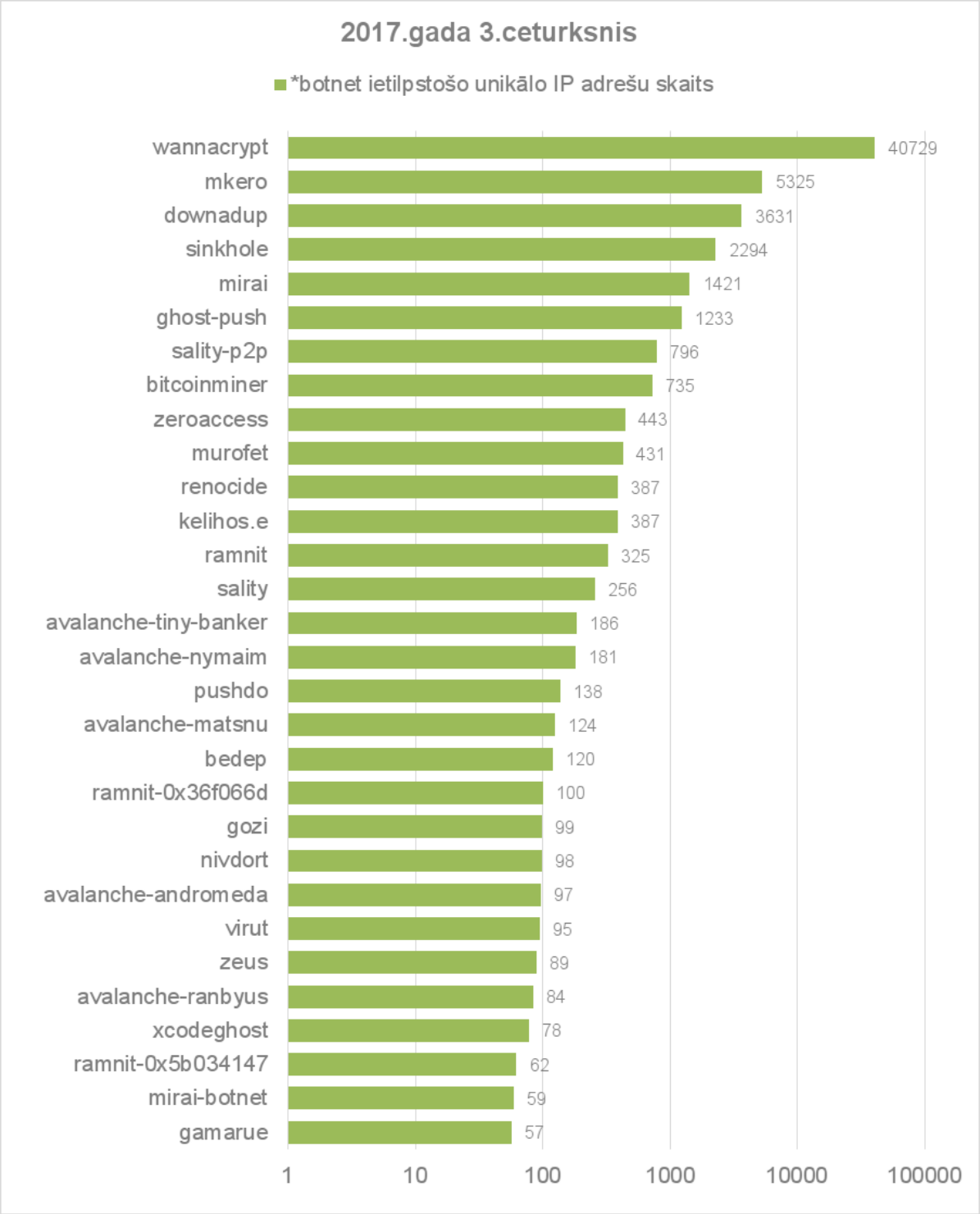
3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 3. ceturksnī pa apdraudējumu veidiem.

Izplatītākais apdraudējuma veids pārskata periodā bija konfigurācijas nepilnības, otrs izplatītākais bija ļaundabīgs kods, bet trešais - ielaušanās mēģinājumi.



4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 3. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

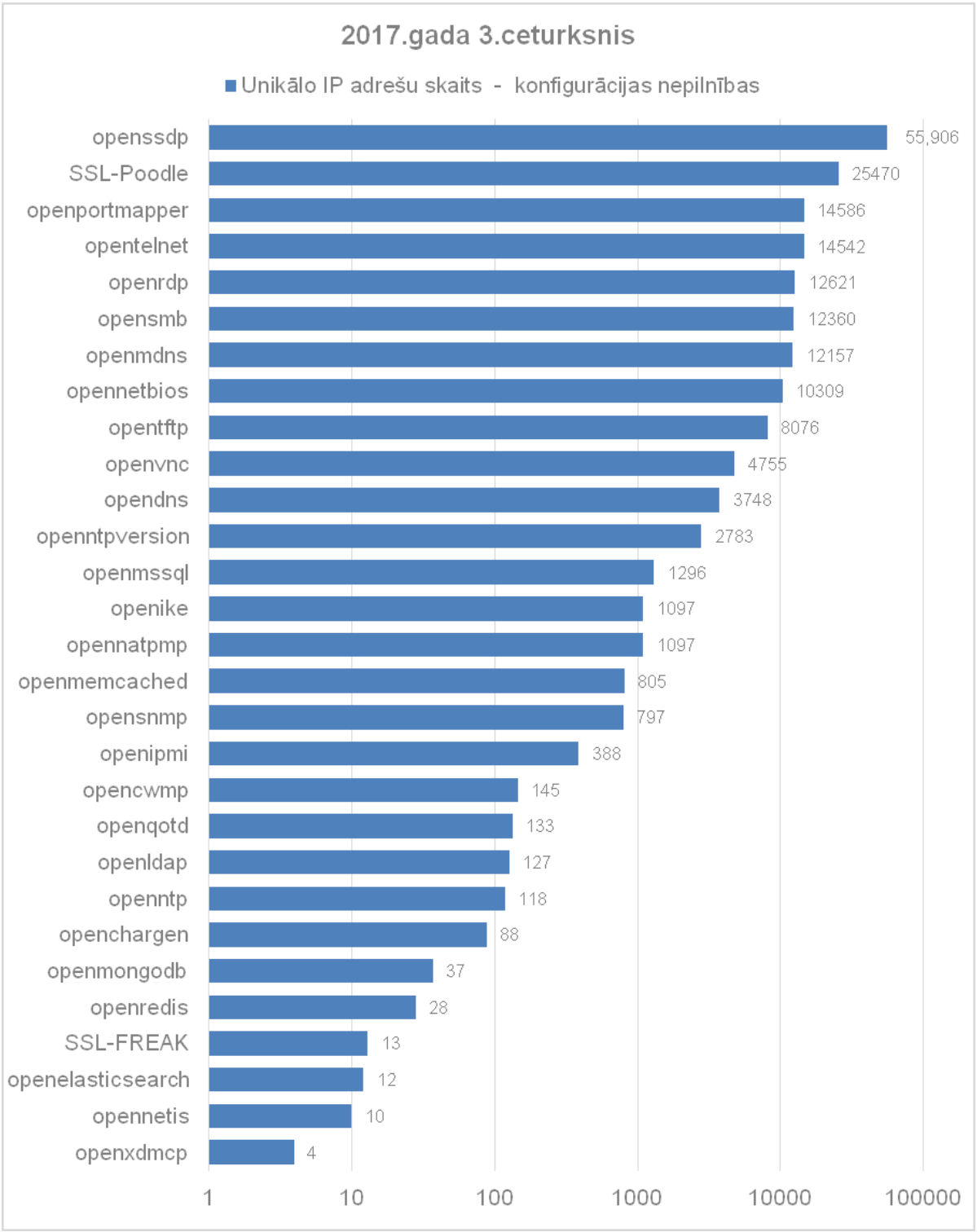
Pirmo vietu ļaunatūras izplatības topā šajā ceturksnī stabili ieņem *botnet* ļaundabīgā koda grupa; tās detalizēts atšifrējums redzams 4.1.grafikā.



4.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 3. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods/ *botnet*.

4.1. attēls parāda, ka augsti izplatības rādītāji joprojām ir ļaunatūrai *WannaCry* jeb *WannaCrypt* – pārskata periodā salīdzinājumā ar iepriekšējo periodu tās apjomi ir dubultojušies. Arī šajā ceturksnī otro vietu ļaunatūras izplatības topā ieņēma *MKero Android* trojānis, kas spēj apiet *CAPCHA* autentifikācijas sistēmu un, lietotājam nezinot, veic lietotāja parakstīšanos uz dažādiem maksas servisiem.

Vietu topa augšgalā nemainīgi saglabā *Conficker*, kaut arī tā ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra.



5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 3. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Opensmb, kas pagājušajā ceturksnī konfigurācijas nepilnību topā bija jaunpienācēja, jau ierindojas sestajā vietā. Šī diezgan plaši izplatītā konfigurācijas nepilnība bija vainojama tādu šifrējošo izspiedējvīrusu kā *WannaCry* un *NotPetya* straujajā izplatībā.

Lai samazinātu kopējo apdraudēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvija Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar interneta pakalpojumu sniedzējiem (IPS), kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs" un informēt savus klientus par to iekārtās konstatētajiem apdraudējumiem. Atbildīgo IPS kopskaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

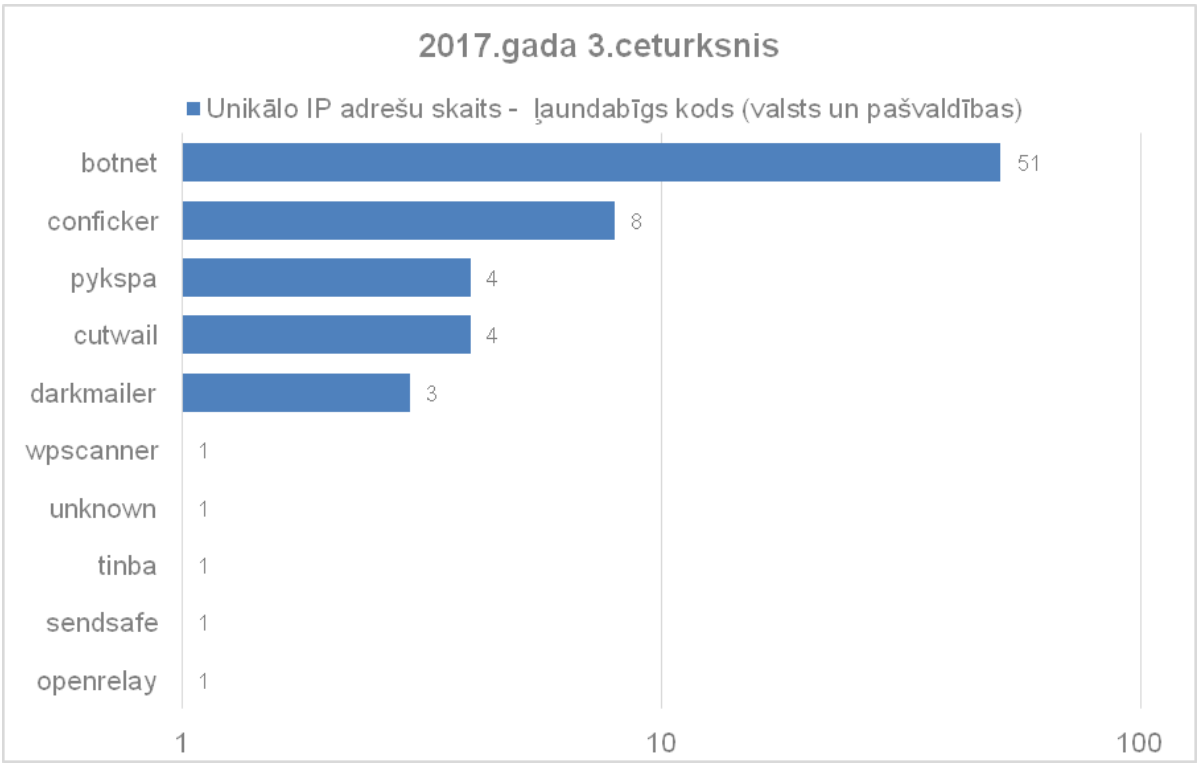
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

CERT.LV apkopo informāciju no valsts un pašvaldību institūcijām par to izmantotajām IP adresēm un tīmekļa vietnēm, lai CERT.LV varētu operatīvāk reaģēt šo iestāžu IT drošības incidentu gadījumos. CERT.LV informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā apdraudētas.

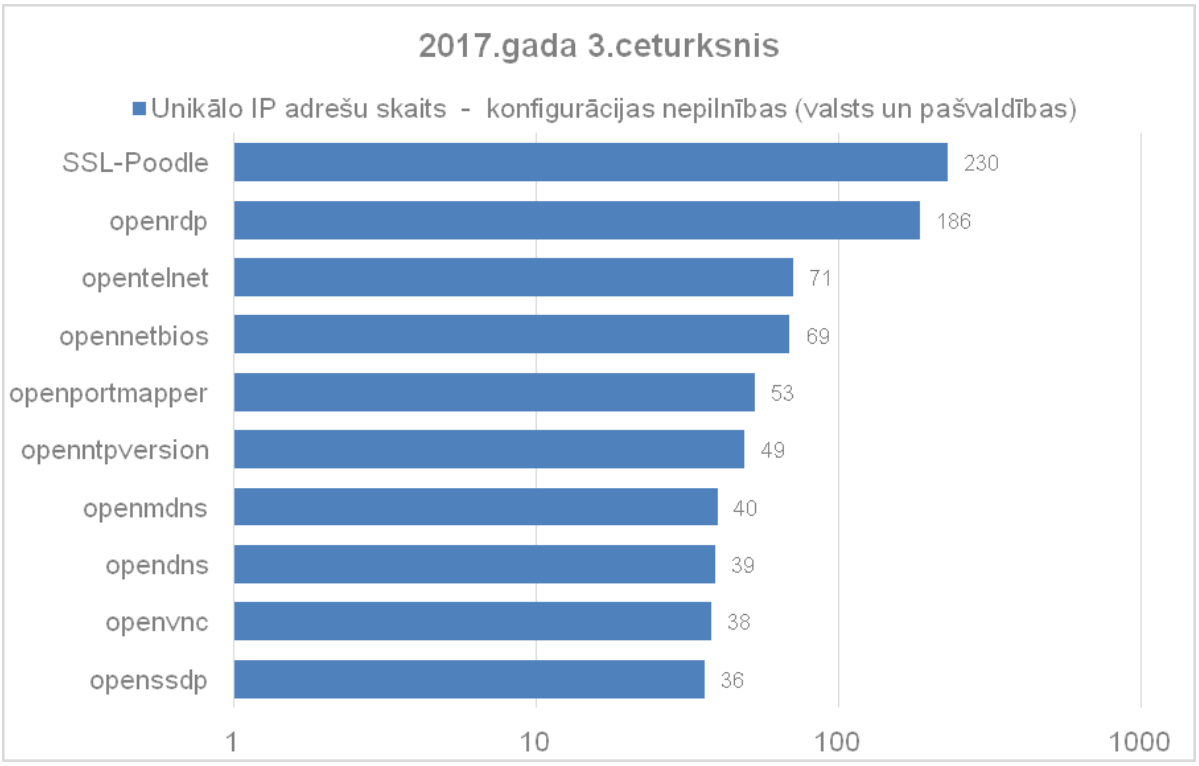
Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:

6.attēls – Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2017. gada 3. ceturksnī.

Kopējais saņemto ziņojumu apjoms par valsts un pašvaldību iestāžu apdraudētajām IP adresēm pārskata perioda noslēgumā samazinājās, samazinoties saņemto ziņojumu apjomam no viena konkrēta ziņojumu avota. Tas vizuāli novērojams arī 6. attēlā. Šīs izmaiņas nav uzskatāmas par indikatoru kopējās situācijas izmaiņai.



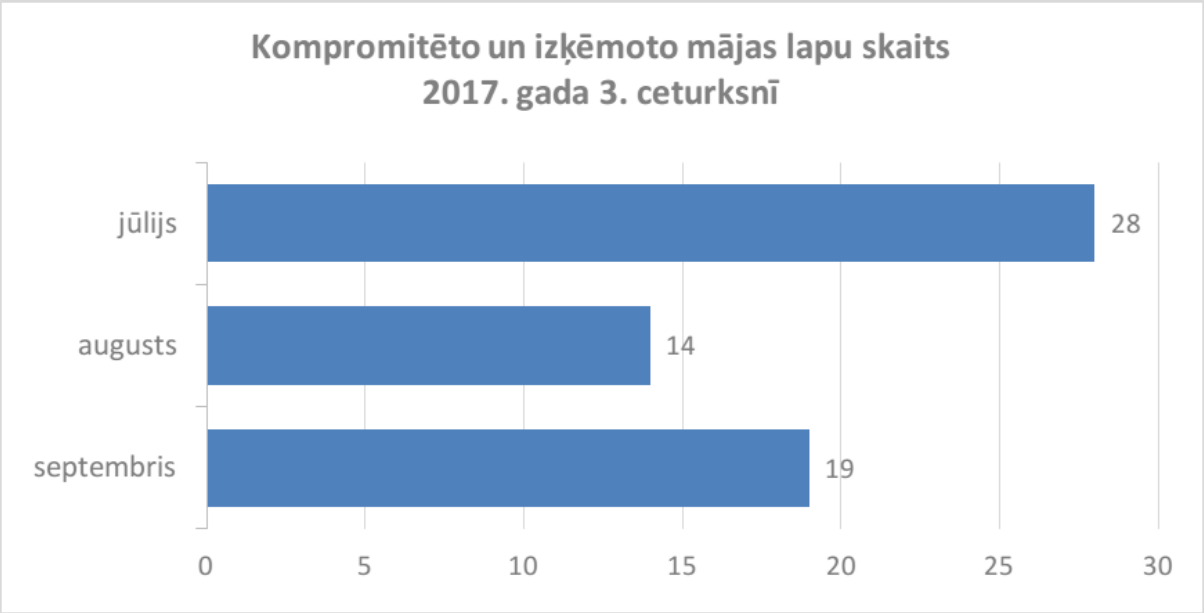
7.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2017. gada 3. ceturksnī ar apdraudējuma veidu – Ļaundabīgs kods (TOP 10).



8.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2017. gada 3. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība (TOP 10).

Salīdzinoši lielais konfigurācijas nepilnību apjoms ir tādēļ, kas vienā ievainojamā IP adresē bieži vien ir sastopami vairāki apdraudējumi – vienā iekārtā vienlaicīgi esošas dažādas konfigurācijas nepilnības.

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksēta 61 kompromitēta un izķēmota tīmekļa vietne. No visām izķēmotajām vietnēm 57 gadījumos vietnes uzturēšanai tika izmantota *Linux* operētājsistēma, 2 gadījumos *Windows*, 1 gadījumā *FreeBSD*, bet 1 gadījumā par izmantoto operētājsistēmu nav informācijas. Sešas no visām pārskata periodā izķēmotajām tīmekļa vietnēm pēdējā gada laikā izķēmotas atkārtoti.



9.attēls – Kompromitēto un izķēmoto tīmekļa vietņu skaits pa mēnešiem 2017. gada 3. ceturksnī.

CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā.

Svarīgākie CERT.LV risinātie drošības incidenti pārskata periodā:

- 02.07. CERT.LV saņēma ziņu, ka kādā tīmekļa vietnē ir publiski pieejams sistēmas konfigurācijas fails. Šāda faila pieeja no interneta rada risku datu noplūšanai un sistēmas kompromitēšanai, tāpēc CERT.LV aicināja ierobežot tam piekļuvi no publiskā tīkla. Piekļuve tika ierobežota.
- 11.07. Tika saņemts ziņojums no kāda uzņēmuma par krāpniecisku e-pastu pareizā latviešu valodā, kas tika sūtīts it kā uzņēmuma vadītāja vārdā ar aicinājumu veikt steidzamus bankas pārskaitījumus. Ticamību raisīja labā latviešu valoda, taču uzņēmuma pārstāvji krāpniecību laikus atpazina un finansiāli zaudējumi nodarīti netika. Līdzīgus e-pastus angļu valodā uzņēmums saņem ik dienu.
- 13.07. Tika saņemts ziņojums no kādas valsts iestādes par krāpniecisku e-pastu it kā valsts iestādes darbinieka vārdā, kas informēja par nepieciešamību atjaunināt piekļuvi e-pasta kontam. Lai to paveiktu, e-pasta saņēmējs tika aicināts sekot saitei un ievadīt datus krāpnieciskā vietnē. Vietnes uzturētāji tika brīdināti par vietnes izmantošanu pretlikumīgām aktivitātēm un aicināti pikšķerēšanas formu aizvērt. Forma tika aizvērta.
- 17.07. Tika saņemta informācija no citas Eiropas valsts CERT vienības par Latvijas IP adresēm, kurās konstatēta *openDNS* konfigurācijas nepilnība un kuras tiek izmantotas DDoS uzbrukumā. Adrešu turētāji tika apzināti un informēti.

- 24.07. Tika saņemts ziņojums no kādas valsts iestādes par krāpniecisku e-pastu, kas sūtīts latviešu valodā it kā iestādes darbinieka vārdā ar aicinājumu veikt steidzamu bankas pārskaitījumu. Krāpnieciskajā e-pastā novērojami sociālās inženierijas elementi un inovatīva pieeja „@" simbola izmantošanai, izveidojot krāpniecisko e-pasta adresi „vārds.uzvārds@iestāde"@intel-mails.cba.pl un novēršot lasītāja uzmanību tikai uz pirmo adreses daļu, tādejādi palielinot uzticamību. Krāpniecība tika atpazīta, zaudējumi nodarīti netika.
- Augustā no vairākiem uzņēmumiem un valsts iestādēm tika saņemti ziņojumi par krāpnieciskiem e-pastiem ar aicinājumu veikt steidzamu maksājumu 44 000 eiro apmērā. Visi e-pasti tika identificēts kā CEO krāpšana, zaudējumi netika nodarīti. Krāpnieciskajos sūtījumos izmantota e-pasta adrese offices.mail1@aol.co.uk.
- 01.08. Saņemts lūgums palīdzēt atpazīt, vai interneta vietne http://eubikestore.com ir krāpnieciska. Lietotājs atzina, ka piedāvājums tīmekļa vietnē ir neticami labs, bet vietne izskatoties pārliecinoši. Pārbaude apliecināja vietnes krāpniecisko raksturu, un lietotājam tika ieteikts nekādā gadījumā neievadīt vietnē savus datus.
- 02.08. Tika saņemts ziņojums no lietotāja par krāpniecību, izmantojot finanšu platformu *Grand Capital META4*. Lietotājam kopumā nodarīti zaudējumi 2600 eiro apmērā. Uzsākot darbību platformā, platformas brokeris aicinājis lietotāju ieskaitīt platformā 1000 eiro, solot atbilstoša apmēra līdzmaksājumu. Nepilnu minūti pēc tam, kad abas puses bija veikušas maksājumus, platformā tika atvērti divi darījumi, kuru rezultātā no lietotāja platformas konta tika noskaitīti gan tikko iemaksātie 2000 eiro, gan vēl 600 eiro, kas radīja negatīvu bilanci 600 eiro apmērā. Lietotājs vērsās pie platformas uzturētājiem ar lūgumu atrisināt situāciju, bet saņēma atteikumu. Jāpiebilst, ka pēc brokera rekomendācijas lietotājs nemainīja paroles un saglabāja tās, lai nevajadzētu katru reizi ievadīt no jauna. CERT.LV ieteica lietotājam vērsties policijā, jo ir radīti materiāli zaudējumi, kā arī pirms akciju tirdzniecības platformu izmantošanas aicina pārliecināties, ka izvēlētais pakalpojuma sniedzējs ir saņēmis Finanšu un kapitāla tirgus komisijas (FKTK) licenci, jo tikai pie šādiem noguldījumu piesaistītājiem klientu aizsargā valsts. Informācija par licencētām ieguldījumu pakalpojumu sniedzējiem Latvijā ir pieejama FKTK mājas lapā – Licencētie pakalpojumu sniedzēji (http://www.fktk.lv/lv/tirgus-dalibnieki/finansu-instrumentu-tirgus/ieguldijumu-pakalpojumu-sniedz.html).
- 03.08. Kāda Latvijas privātpersona saņēma zvanu no Norvēģijas numura. Zvanītājs stādījās priekšā kā Microsoft pārstāvis un teica, ka datoram vajag apmaksāt sertifikātu, lai dators nesūtītu kļūdu paziņojumus. Microsoft "pārstāvis" minēja, ka samaksa par sertifikātu ir tikai desmit kronas, bet apmaksa jāveic konkrētā tīmekļa vietnē.

  Rezultātā privātpersona ievadīja krāpnieciskā vietnē savas bankas kartes datus. Privātpersona tā sauktajam „pārstāvim" papildus ļāva uzinstalēt uz sava datora *TeamViewer* un *RegSupreme* pārvaldības programmu, tādā veidā nododot ļaundarim kontroli pār datoru.

  Pēc telefonsarunas no lietotāja konta tika aizskaitīti 3000 eiro. Cietušais nekavējoties sazinājās ar savu banku un paziņoja par krāpniecību. Diemžēl lietotājs nepiefiksēja krāpnieciskās vietnes adresi, kurā vadījis savus kartes datus. Lapas adrese neuzrādījās arī vēsturē. Pagaidām cietušajam naudu nav izdevies atgūt. Ņemot vērā apstākļus, tika ieteikts rakstīt iesniegumu Norvēģijas policijā.

- 04.08. Tika saņemts ziņojums no kāda uzņēmuma par krāpniecisku e-pastu uzņēmuma vadītāja vārdā ar aicinājumu veikt steidzamu bankas pārskaitījumu. Krāpniecība tika atpazīta pēc nekorektās Reply-To adreses.
- 05.08. Kāds lietotājs lūdza palīdzību nesankcionētu ziņu apturēšanā viņa profilā sociālajā tīklā *Facebook*. Nesankcionētās ziņas no profila, izmantojot *Facebook Messenger*, tika nosūtītas arī lietotāja draugiem. CERT.LV ieteica pārbaudīt lietotnes, kurām atļauta piekļuve *Facebook* profilam un sniegtas tiesības publicēt ziņas lietotāja vārdā, kā arī pārbaudīt iekārtu, vai tajā nav vīruss. Pēc CERT.LV ieteikumiem lietotājam izdevās problēmu novērst.
- 09.08. Kāda valsts iestāde piedzīvoja vairākus ilgstošus uzbrukumus iestādes e-pasta serverim. Vienā uzbrukuma reizē e-pasta serveris saņēma 2000 kaitnieciskus sūtījumus. Ugunsmūra risinājums visus kaitīgos e-pastus bloķēja. Uzbrukumi tika veikti no daudzām savstarpēji nesaistītām IP adresēm dažādās pasaules valstīs, kas norāda, ka uzbrukumā iesaistīts inficētu iekārtu robotu tīkls jeb *botnets*. Dažas uzbrukumā iesaistītās IP adreses bija arī no Latvijas.
- 10.08. Tika saņemts lūgums veikt drošības testu kādas valsts iestādes tīmekļa vietnēm un tīmekļa servisiem. Testu rezultātā tika konstatētas vairākas nepilnības, viena no tām kritiska. Iestādei tika nosūtīts ziņojums par testa rezultātiem un ieteikumi nepilnību novēršanai.
- 11.08. Tika saņemts ziņojums no kāda uzņēmuma par šifrējošā izspiedējvīrusa *Scarab ransomware* uzbrukumu uzņēmuma serveriem. Uzbrukuma rezultātā tika sašifrēta daļa failu. Tiek pieļauts, ka izspiedējvīruss izplatījās, izmantojot SMB failu apmaiņas protokolu. Gan kompānijas izmantotajiem *Windows* datoriem, gan serverim bija jaunākie atjauninājumi. Faili tika atjaunoti no rezerves kopijām.
- 11.08. Kāds uzņēmums ziņoja par šantāžas mēģinājumu. Uzņēmums saņēma e-pasta vēstuli, kuras sūtītāji uzdevās par grupējumu *Kadyrovtsy* un draudēja ar 600 Gbps jaudas DDoS uzbrukumu, ja uzņēmums neveiks samaksu kriptovalūtā 2 bitcoin apmērā. Uzņēmums nepakļāvās šantāžai, bet uzstādīja nepieciešamos drošības rīkus. Uzņēmuma infrastruktūra piedzīvoja nelielus iebiedēšanas uzbrukumus, bet reāls DDoS uzbrukums nesekoja.

  Šis nav pirmais gadījums, kad uzbrucēji izsaka draudus, kaut arī reālu uzbrukumu nav gatavi veikt, cerot, ka iebiedēšana būs gana efektīva un upuris izvēlēsies maksāšanu kā labāko aizsardzību.
- 11.08. Kāda valsts iestāde ziņoja par kārtējo atklāto krāpniecisko tīmekļa vietni, kuras dizains un pretlikumīgi izmantotais valsts ģerbonis maldināja vietnes apmeklētājus, liekot domāt, ka šī ir oficiāla valsts iestādes mājas lapa un tajā publicētais saturs ir ticams. Pēc CERT.LV brīdinājuma no vietnes tika izņemta oficiālā valsts simbolika un novērsta vietnes maldinošā asociācija ar valsts institūciju.
- 14.08. Kāda valsts iestāde ziņoja par 12 stundu ilgu *botnet* uzbrukumu iestādes e-pasta serverim. Ugunsmūra risinājums šos uzbrukumus sekmīgi atvairīja.

- 15.08. Tika saņemta ziņa no kāda lietotāja par krāpniecību iepazīšanās vietnē be2.de. Klients bija saņēmis e-pastu, kurā draudēts ar policiju un tiesas darbiem, ja norādītais parāds 309.80 eiro apmērā netiks apmaksāts. Analizējot situāciju, izrādījās, ka lietotājs bija piereģistrējies tīmekļa vietnē, un vēlāk par šo vietni aizmirsis, bet vietne automātiski veica VIP statusa pagarināšanu. CERT.LV iesaka rūpīgi iepazīties ar visiem lietošanas noteikumiem, pirms piekrist jebkuras tīmekļa vietnes izmantošanai, kā arī apturēt servisa abonēšanu vai dzēst profilu, tiklīdz to pārtrauc lietot.
- 15.08. Saņemta ziņa no kādas organizācijas par krāpniecisku e-pastu ar aicinājumu veikt starptautisku maksājumu uz Itāliju 35,509,00 eiro apmērā. Krāpniecība atpazīta pēc neatbilstošas e-pasta adreses info@predsedapredstavenstva.ml. Zaudējumi un kaitējums netika nodarīts.
- 15.08. No kāda uzņēmuma tika saņemta informācija par 215 saņemtiem kaitīgiem e-pastiem, kuros lūgts sniegt tāmi pielikumā norādītajām pozīcijām. Pielikumā atradās arhīva fails .ZIP formātā, kas saturēja *JAR* ļaunatūru.
- 17.08. Kādas valsts iestādes portāls piedzīvoja masveida uzbrukumu. Tajā bija iesaistītas virkne dažādu IP adrešu, no tām viena bija no Latvijas. No visām IP adresēm tika veikti līdzīgi pieprasījumi ar mērķi izgūt datus. Neviens uzbrukuma mēģinājums nebija veiksmīgs, visi tika atvairīti.
- 17.08. Tika saņemta informācija no citas valsts CERT vienības par kādas programmatūras ievainojamību un lietotājiem Latvijā, kuri, iespējams, lieto ievainojamo programmatūras versiju un ir pakļauti uzbrukumu riskam. Aicinājumā apziņot apdraudētos lietotājus tika iekļauta informācija par nepieciešamajiem atjauninājumiem, lai apdraudējumu novērstu. CERT.LV sazinājās ar programmatūras lietotājiem Latvijā, informējot tos par apdraudējumu un aicinot veikt atjauninājumus.
- 21.08. Saņemts ziņojums par bērnu pornogrāfiju saturošu materiālu izplatīšanu. Informācija tika nodota drossinternets.lv ziņojumu centram un ievietota INHOPE datu bāzē tālākai apstrādei.
- 21.08. Tika saņemts ziņojums no kādas valsts iestādes par viltotu iestādes tīmekļa vietni, kas tiek izmantota krāpnieciskos nolūkos. Pārkāpums tika pieteikts vietnes uzturētājiem. Oficiālā atribūtika, kas maldinoši asociēja vietni ar iestādi, no vietnes tika izņemta.
- 01.09. Saņemta ziņa par krāpniecību sociālajos tīklos. Lietotāji tika uzrunāti no viltus profila it kā ar mērķi iepazīties, bet vēlāk tika mēģināts tos iežēlināt ar stāstiem par atrašanos kara zonā un izteikts aicinājums pārskaitīt naudu. CERT.LV ieteica vērsties ar iesniegumu policijā.
- 08.09. No kāda uzņēmuma tika saņemta informācija par krāpniecisku e-pastu ar brīdinājumu, ka e-pasta pakalpojumu nodrošinātājam ir „bijis sistēmas jauninājums serveros" un „ņemot vērā neseno kontu zādzību un nozaudēšanas pieaugumu" lietotāji tiek aicināti sekot saitei un atjaunināt savu e-pasta kontu, ievadot piekļuves informāciju. E-pasts tika noformēts diezgan labā latviešu valodā, norādot salīdzinoši ticamus iemeslus konta pārbaudei. CERT.LV nav informācijas, ka kāds šajā pikšķerēšanas kampaņā būtu cietis. Pikšķerēšanā izmantotā uzlauztā tīmekļa vietne tika salabota.
- 08.09. Tika saņemta informācija par iespējamu ļaunatūras komand- un kontrolcentru. Lieta tika nodota Valsts policijai.

- 27.09. Tika uzlauzta un izķēmota kāda novada tīmekļa vietne. Vietnes uzturētāji tika informēti. Vietne tika uzlauzta, jo izmantoja novecojušu satura vadības sistēmas *Joomla* versiju. Pēc brīdinājuma vietne tika salabota.
- 27.09. Tika saņemta ziņa no kāda uzņēmuma pārstāvja par šifrējošo izspiedējvīrusu *Locky* darbinieka datorā. Pārstāvis lūdza palīdzību atgūt sašifrētos failus. Vīruss tika iedarbināts, atverot e-pasta pielikumu. CERT.LV ieteica nākotnē izmantot *Windows AppLocker*, kas kontrolētu, kurš un no kurienes var atvērt izpildāmos failus. Tāpat CERT.LV brīdināja par to, ka samaksāšana negarantē failu atgūšanu un nākotnē iesakāms parūpēties par rezerves kopijām.

CERT.LV pasākumi incidentu novēršanai:

- Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta CERT.LV sagatavotajās nedēļas ziņās un sociālā tīkla Twitter kontā (@certlv).

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 6. punktā.

3. Mobilo ierīču ļaunatūras pētniecība.

Mobilā ļaunatūra kļūst arvien aktuālāks apdraudējums. Par to liecina gan CERT.LV saņemtie ziņojumi, gan sabiedrības un mediju interese par mobilo ierīču drošības jautājumiem, gan arvien pieaugošais mobilo ierīču skaits, kas pie CERT.LV speciālistiem nonāk Datorologa akciju laikā.

Tika saņemtas vairākas ziņas ar sūdzībām par neautorizētām ziņām *Facebook* profilā, kas tālāk draugu lokam izplatījās, izmantojot *Facebook Messenger*. Daži izplatītie ziņojumi saturēja arī kaitnieciskas saites, kas paredzētas ļaunatūras izplatīšanai. Draugu lokam no inficētā profila šīs saites tika nosūtītas ar uzaicinājumu aplūkot interesantu video. Nesankcionētu ziņu parādīšanās profilā visbiežāk izraisīja neapdomīga aplikāciju instalēšana, sniedzot šīm aplikācijām piekļuves atļauju savam *Facebook* profilam ar tiesībām veikt ierakstus profila īpašnieka vārdā.

Pārskata periodā tika saņemtas informācija par *Android* lietotājus apdraudošu ļaunatūru *Invisible Man*, kas uzdevās par *Flash* atjauninājumiem. Ļaunatūra veica lietotāja ievadīto datu nolasīšanu (*keylogging*) ar mērķi iegūt paroles un bankas piekļuves datus. Ļaunprogrammatūra pirms darbības uzsākšanas veica viedtālruņa valodas iestatījumu pārbaudi. Ja iestatītā valoda bija krievu, ļaunatūra pārtrauca savu darbību. Citos gadījumos programma lūdza atļauju izmantot pieejamības pakalpojumus (*accessibility services*) un instalēja sevi kā noklusējuma īsziņu lietotni.

CERT.LV saņēma arī ziņojumus par *MKero Android* trojāni, kas, apejot *Google* drošības pasākumus, ar dažādām spēlēm un lietotnēm nokļuva oficiālajā *Google Play*. *MKero* spēj apiet *CAPCHA* autentifikācijas sistēmu un, nonākot lietotāja ierīcē, veic lietotāja parakstīšanos uz dažādiem maksas servisiem.

4. Rekomendācijas par informācijas tehnoloģiju risku novēršanu (komunikācija ar sabiedrību).

Informācija par CERT.LV sadarbību ar medijiem

Pārskata periodā bija vērojama mediju interese par krāpniecības gadījumiem sociālajos tīklos un kiberuzbrucēju aktivitāti Krievijas un Baltkrievijas apvienoto mācību „Zapad 2017" laikā.

Informācija par CERT.LV tīmekļa vietnēm:

https://www.cert.lv publicētas 19 ziņas. Populārākā bija ziņa par kiberdrošības konferenci "Kiberšahs 2017" ar 2754 unikāliem skatījumiem. Otra populārākā bija ziņa par krāpniecisku saišu izplatīšanu sociālajā tīklā *Facebook*, kuru skatījuši 1232 unikāli apmeklētāji. Trešā populārākā bija Kontaktu sadaļa ar 1077 unikāliem skatījumiem. Kopā CERT.LV mājas lapai bijuši 14 567 lapu skatījumi, kurus veido 8 910 unikāli lapu skatījumi.

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 11 797 apmeklējumi, no tiem 9 001 unikāls apmeklējums. CERT.LV turpina tulkot un portālā a izdevumus (Informācijas drošības biļetens, ko sagatavo SANS institūts).

Portālā esidross.lv publicētie raksti:

- Tiešsaistes spēļu drošība
- Rezerves kopijas un atgūšana
- Paroļu pārvaldnieki

CERT.LV sociālo tīklu konti:

- Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1815.
- CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 718.
- CERT.LV draugiem.lv profila http://www.draugiem.lv/certlv sekotāju skaits pārskata perioda beigās bija 73.

5. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

21. jūlijā CERT.LV pārstāvis tikās ar Swedbank, lai sagatavotu izglītojošu materiālu par dažādiem kiberdrošības jautājumiem, kas skar uzņēmumus (paroles, šifrējošie izspiedējvīrusi u.c.).

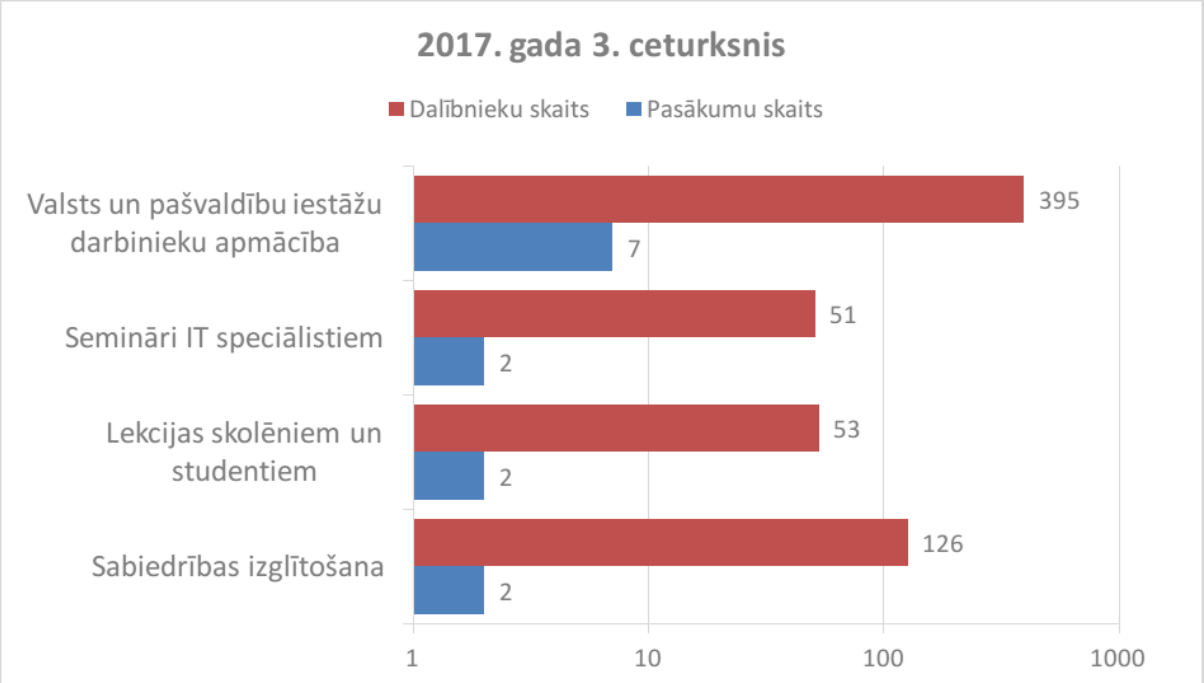
28. augustā notika tikšanās ar NetSafe Latvia drošāka interneta centru, lai vienotos par aktivitātēm oktobrī – Eiropas Kiberdrošības mēneša laikā.

4. septembrī notika tikšanās ar Swedbank, lai pārrunātu iespējamo sadarbību izglītojošu aktivitāšu jomā.

12. septembrī CERT.LV pārstāvis piedalījās Erasmus+ programmas stratēģisko skolu sadarbības partnerības projekta "The ICT road to STEM through TCC" sanāksmē un sniedza prezentāciju par CERT.LV izmantotajiem materiāliem 1.-6. klašu skolēnu izglītošanai par IT drošību. CERT.LV pārstāvis piedalījās arī diskusijā un informācijas apmaiņā par mazāko klašu skolēnu izglītošanu.

27. septembrī notika tikšanās ar Vidzemes augstskolas pārstāvjiem par iespējamo sadarbību maģistratūras studentu prakses jautājumos.

Pārskata periodā CERT.LV par IT drošību izglītoja 625 cilvēkus, iesaistoties 13 izglītojošos pasākumos.



10.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2017. gada 3. ceturksnī.

6. Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā.

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 13.07., 10.08., 14.09. DEG sanāksmes.
- 19.07. Tikšanās Aizsardzības ministrijā par NIS direktīvas ieviešanas pasākumiem.
- 19.07. Tikšanās Aizsardzības ministrijā ar VARAM un LVRTC, lai pārrunātu eID jautājumus.
- 30.08. Tikšanās Aizsardzības ministrijā, lai vienotos par laika grafiku un uzdevumu sadalījumu, kas veicami pirms NIS direktīvas ieviešanas.
- 29.09. Tikšanās Aizsardzības ministrijā par Kiberaizsardzības vienības darbību.

Sadarbība ar valsts iestādēm incidentu risināšanā aprakstīta atskaites 2. punktā.

7. Valsts un pašvaldību institūciju un elektronisko sakaru komersantu uzraudzība par Informācijas tehnoloģiju drošības likumā noteikto pienākumu veikšanu.

IT drošības likums nosaka, ka valsts un pašvaldību institūcijām jāinformē CERT.LV par nozīmēto atbildīgo personu, kura iestādē īsteno informācijas tehnoloģiju drošības pārvaldību. Līdz 2017. gada 30. septembrim CERT.LV apkopojusi informāciju par 1311 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību vai ar to saistītas.

IT drošības likums un ar to saistītie MK noteikumi Nr. 327 nosaka kārtību, kādā Elektronisko sakaru komersantiem (turpmāk – ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai.

Šī pārskata perioda beigās rīcības plānu statistika ir šāda:

- saņemti 15 atjaunoti ESK rīcības plāni;
- saņemts 21 jauns ESK rīcības plāns;
- 15 ESK rakstiski apliecināja, ka neuztur publisko elektronisko sakaru tīklu.

Pārskata periodā CERT.LV nav saņēmis nevienu ziņojumu no ESK par drošības vai integritātes pārkāpumiem, kas būtiski ietekmējuši elektronisko sakaru tīkla darbību vai pakalpojumu sniegšanu un atbilst Informācijas tehnoloģiju drošības likuma (ITDL) 9.panta pirmās daļas 2.punktam.).

Pārskata periodā CERT.LV nav konstatējis apdraudējumus, kuru atrisināšanai būtu nepieciešams slēgt galalietotājam piekļuvi elektronisko sakaru tīklam (ITDL 9.panta pirmās daļas 5.punkts).

ITDL 6^1 pantā minētie gadījumi aplūkoti atskaites 2. punktā.

8. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 25.-26.07. CERT.LV pārstāvis piedalījās „BSides Las Vegas" konferencē.
- 25.07. CERT.LV komanda piedalījās CTF (Capture the Flaf) tipa mācībās „CyberEx 2017" un 48 komandu konkurencē ieguva 15. vietu.
- 27.-30.07. CERT.LV pārstāvis apmeklēja „DEF CON 25" konferenci Lasvegasā.
- 26.08.-02.09. CERT.LV pārstāvis pasniedza „Malware and Exploitation Essentials" kursu NATO CCDCoE Tallinā.
- 3.-8.09. CERT.LV pārstāvis apmeklēja „CERT-EU 2017 Conference – The Future of Cyber Security in Europe" Briselē un piedalījās paneļdiskusijā par CERT komandu sadarbību Eiropā.
- 11.-15.09. CERT.LV pārstāvis pasniedza „IT Systems Attacks and Defense" kursu NATO CCDCoE Tallinā.
- 12.-13.09. CERT.LV pārstāvis piedalījās TNC2018 konferences programmkomitejas sanāksmē Amsterdamā, Nīderlandē.
- 17.-22.09. CERT.LV pārstāvis pasniedza NATO CCDCoE kursu „IT Systems Attacks and Defense" Lielbritānijā.
- 20.-23.09. Dalība un sesiju vadīšana TF-CSIRT 52.sanāksmē Stokholmā, Zviedrijā.
- 29.09. CERT.LV pārstāvis Tallinā piedalījās Eiropas Kiberdrošības mēneša atklāšanas pasākuma ietvaros notiekošajā paneļdiskusijā par kiberdrošību darbavietā.
- No jūlija līdz septembrim CERT.LV gatavoja projekta pieteikumu „CEF TELECOM CALL FOR PROPOSALS 2017" CEF-TC-2017-2 uzsaukumam. 21.septembrī tika iesniegts pieteikums ar nosaukumu: „Improving Cyber Security Capacities in Latvia".

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

9. Citi normatīvajos aktos noteiktie pienākumi.

- 08.09. Notika tikšanās ar Huawei pārstāvjiem par iespējamo sadarbību sabiedrības izglītošanas.
- 29.-30.09. CERT.LV pārstāvji apmeklēja „The Riga Conference 2017".

10. Ar Elektroniskās identifikācijas uzraudzību saistīto pienākumu izpilde.

Saskaņā ar MK 2015. gada 3. februāra sēdes protokolā Nr. 6 27. §, ar kuru pieņemts zināšanai informatīvais ziņojums "Par kompetento un atbildīgo iestādi, kura nodrošinās kvalificētu un kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzību" noteikto CERT.LV pārskata periodā turpināja noteikto funkciju veikšanu.
Iepriekšminēto funkciju izpildei veikto darbu uzskaitījums:

- CERT.LV pārstāvji piedalījās elektroniskās identifikācijas komitejas sēdē, kuras laikā saskaņoja Latvijas Valsts radio un televīzijas centra darbības izbeigšanas plānu.
- CERT.LV pārstāvji piedalījās starpinstitucionālā sanāksmē par trīs Ministru kabineta noteikumiem, kuri sagatavoti, pamatojoties uz Fizisko personu elektroniskās identifikācijas likumu.
- CERT.LV sadarbībā ar Aizsardzības ministrijas speciālistiem aktīvi iesaistījās komitejas darbā, kas saistīts ar tīmekļa vietnes sadaļas izveidi, tās struktūru un saturu, lai turpmāk sniegtu informāciju, kas saistīta ar uzticamības pakalpojumu sniedzēju uzraudzību un pašlaik pieejama Datu valsts inspekcijas tīmekļa vietnē.
- CERT.LV pārstāvji piedalījās Eiropas Komisija organizētā vebinārā par Eiropas Komisijas uzturētā uzticamības pakalpojumu uzticamības saraksta rediģēšanas rīka jautājumiem.
- CERT.LV pārstāvji piedalījās sanāksmē ar Aizsardzības ministrijas pārstāvjiem par Elektroniskās identifikācijas uzraudzības komitejas tīmekļa vietnes saturu.

2017. gada 29. septembrī stājās spēkā Ministru kabineta noteikumi Nr. 577 „Grozījumi Ministru kabineta 2016. gada 1. novembra noteikumos Nr. 695 „Elektroniskās identifikācijas uzraudzības komitejas nolikums", ar kuriem tika izmainīts nosaukums, mainot "Elektroniskās identifikācijas uzraudzības komiteja" uz "Digitālās drošības uzraudzības komiteja.

11. Papildu pasākumu veikšana.

Atskaite par Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centra ziņojumu līnijas darbību.

Latvijas Interneta asociācijas „Net-Safe Latvia" drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.07.2017. līdz 30.09.2017. ir saņēmusi un izvērtējusi 110 ziņojumus. No tiem 54 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 5 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 11 ziņojumos konstatēta personas goda un cieņas aizskaršana, 2 gadījumos konstatēti vardarbīga rakstura materiāli un 7 ziņojumi saņemti par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 6 ziņojumi, 4 ziņojumu saturs nav bijis pretlikumīgs, 21 gadījumā ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 18 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 23 ziņojumi par bērnu seksuālu izmantošanu saturošiem

materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Sagatavotājs – Līga Besere
Tālrunis: 67085888
E-pasts: liga.besere@cert.lv